Group Diffie-Hellman Key Exchange

Secure Against Dictionary Attacks

Olivier Chevassut

(Ernest Orlando Lawrence Berkeley National Lab)

Emmanuel Bresson and David Pointcheval

(École normale supérieure)

Outline

- Motivation

- Setting

- Related Work

- Model of Security

- Definitions of Security

- A Protocol for Password-Based Key Exchange

- Theorem of Security

- Conclusion

Motivation

- An increasing number of mobile applications need to communicate within small groups, e.g.

  — conferencing and meeting

  — personal networking

  — emergency rescue and military operations

- An increasing number of mobile applications have security requirements

  — data privacy and integrity

  — protection from hackers

  — protection from viruses

- Mobile group communication must address security needs

Setting

- **Member characteristics**

  — relatively small group (up to 100 members)

  — members have similar compute power

  — no hierarchy among members (no client/server model)

- **Environmental constraints**

  — no security infrastructure

  — no fixed networking infrastructure

  — multicast communication capabilities

Prior Work

- "Provably Authenticated Group DH Key Exchange", ACM CCS'01

  — a small number of users gather to form a group

  — public-key infrastructure

  — treatment in the framework of provable security

  — a provably secure protocol for authenticated group DH key exchange

How Provable Security works

1. Specification of a model of computation
- instances of players are modeled via oracles
- adversary controls all interactions among the oracles
- adversary's capabilities are modeled by queries to the oracles
- adversary plays a game against the oracles

2. Definition of the security goals
- authentication, freshness and secrecy of session keys, forward-secrecy
- security against dictionary attacks

3. Statement of the intractability assumptions
- group computational/decisional Diffie-Hellman (GCDH/GDDH)

4. Description of the algorithm and its proof of security
- proof shows by contradiction that the algorithm achieves the security goals under the intractability assumptions

Model of Communication

- A set of *n* players
  - — each player is represented by an oracle
  - — each player holds a low-entropy secret (PW)
- A multicast group consisting of a set of players
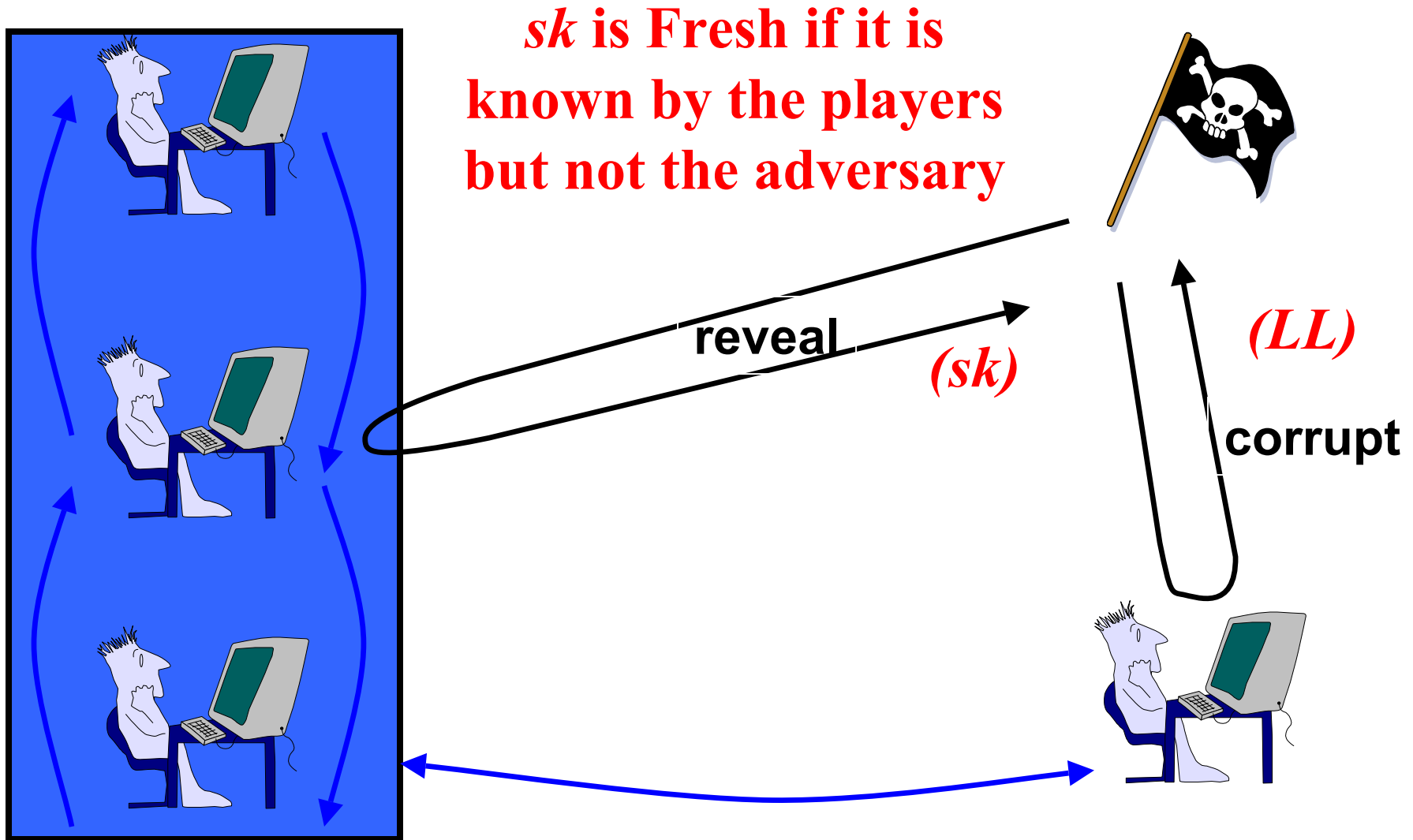

Multicast group with sk
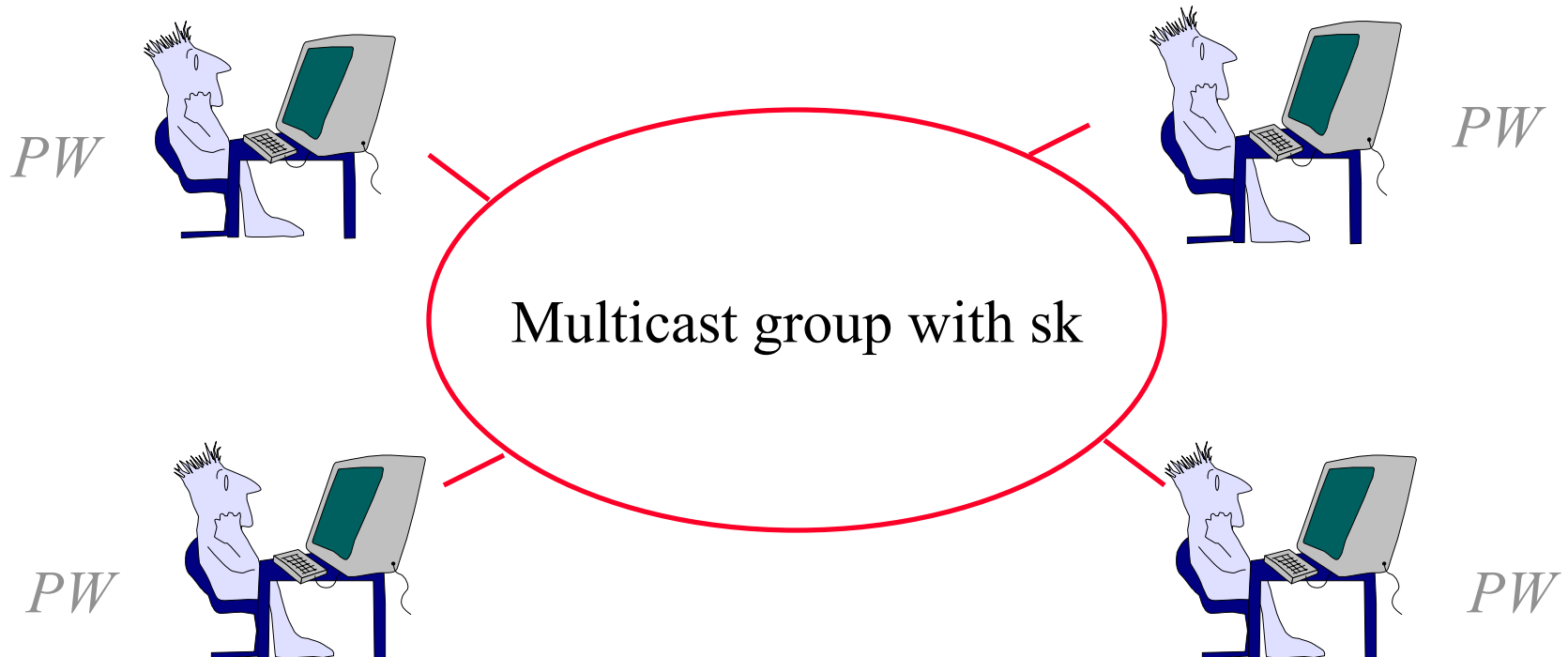
Modeling the Adversary

- Adversary's capabilities modeled through queries
    - send: send messages to instances
    - execute: obtain honest executions of the protocol
    - reveal: obtain an instance's session key
    - corrupt: obtain the value of the password

PW   *PW*   *PW*   *PW*

send   **reveal**   **execute**   **corrupt**
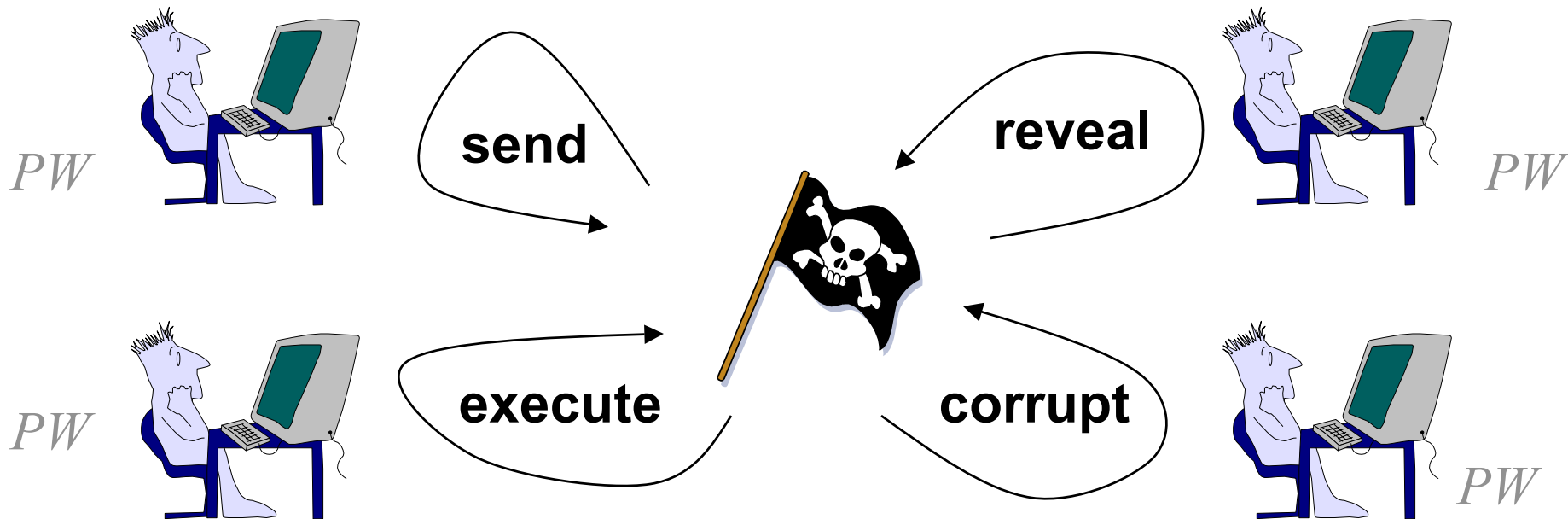
Freshness Related Queries

sk is Fresh if it is known by the players but not the adversary

reveal *(sk)*

(LL)

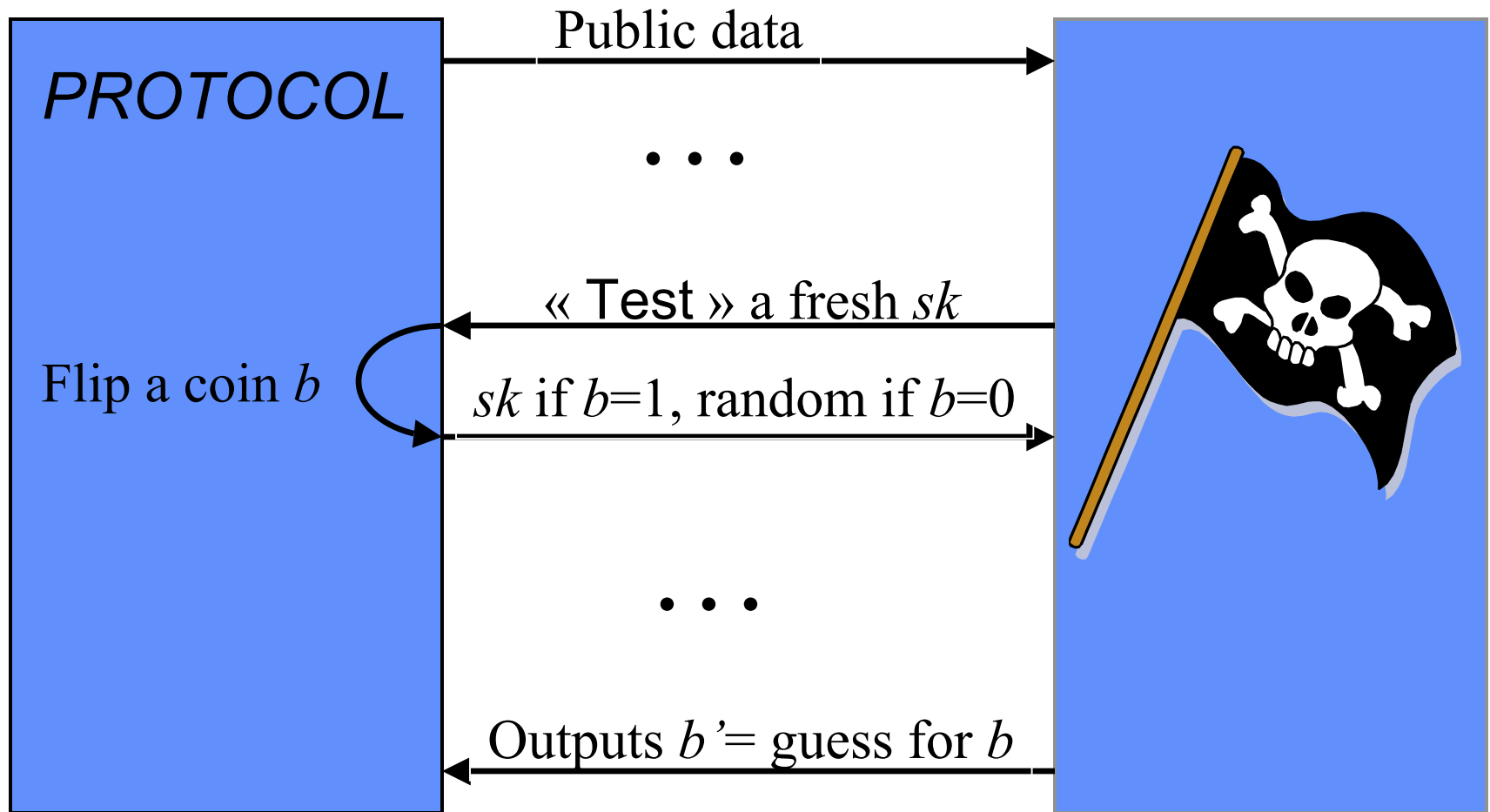**corrupt**

Security Goal : AKE
Authenticated Key Exchange

- **Implicit authentication**

  — only the intended partners can compute the session key

- **Semantic security**

  — the session key is indistinguishable from a random string

  — modeled via a Test-query

- **Security against dictionary attacks**

  — passive eavesdropping does not help the adversary in computing any information about the password

  — only interactions with the instances help the adversary in computing information about the password

Security Definitions (AKE)

PROTOCOL

Public data →

· · ·

« Test » a fresh sk ←

Flip a coin b

sk if $b=1$, random if $b=0$ →

· · ·

Outputs $b' =$ guess for b ←

Intractability Assumption: GCDH Group Computational Diffie-Hellman

- The CDH assumption generalized to the multi-party case
  - — given the values $g^{\prod x_i}$ for some choice of proper subset of $\{1, \ldots, n\}$
  - — one has to compute the value $g^{x_1 \cdots x_n}$

- Example with three parties (*n=3* and *I={1,2,3}*)
  - — given the set of values

$$, \quad g^{x_1} \quad , \quad g$$
$$, \quad g^{x_1 x_2} \quad , \quad g^{x_1} \quad , \quad g^{x_2}$$
$$, \quad g^{x_1 x_2} \quad , \quad g^{x_1 x_3} \quad , \quad g^{x_2 x_3}$$

  - — compute the value $g^{x_1 x_2 x_3}$

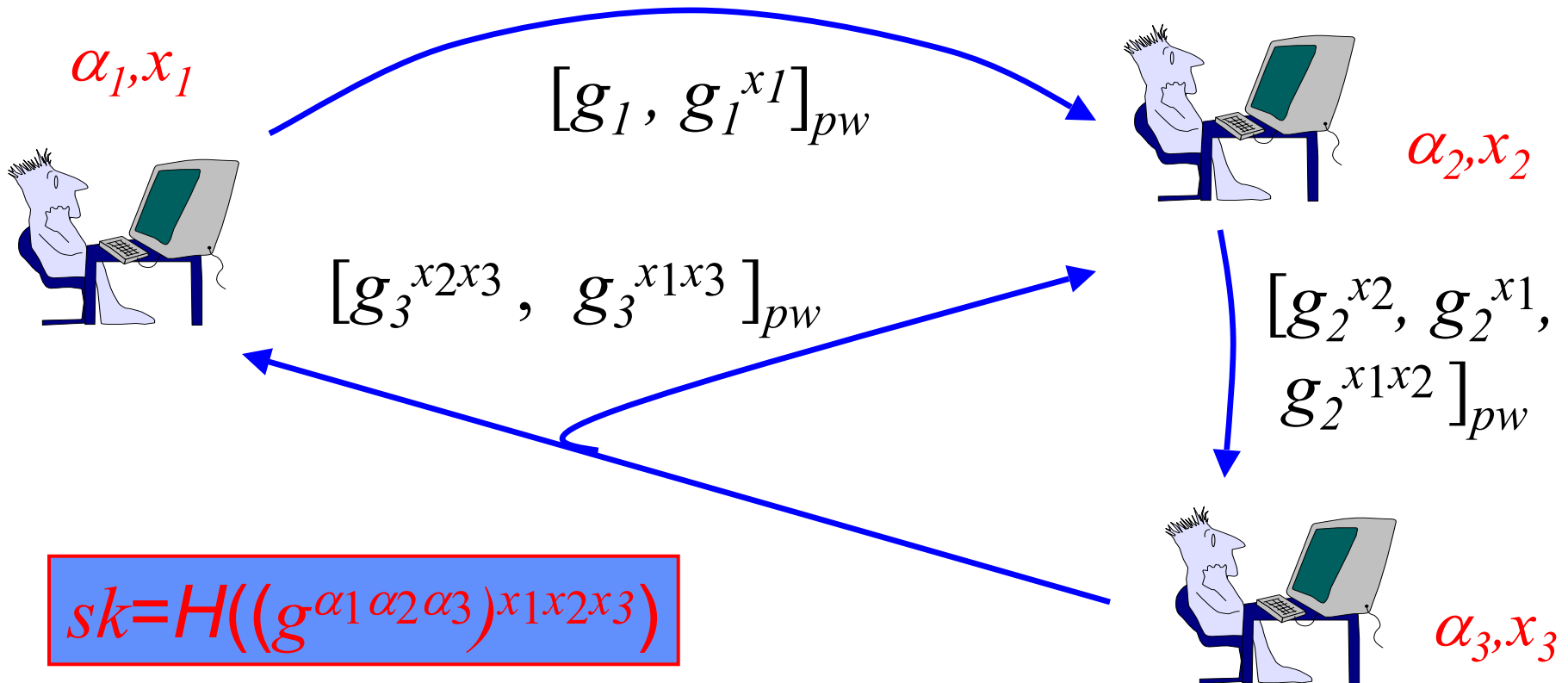- The GCDH is equivalent to both the DDH and CDH, SAC'98

A Protocol for Password-Based Group Key Exchange

- ## The session key is
  - — $sk=H(g^{x_1 x_2 \dots x_n})$

- ## Ring-based algorithm are encrypted under the password
  - — up-flow: the contributions of each instance are gathered

  - — down-flow: the last instances broadcasts the result

  - — instances compute the session key from the broadcast

- ## Many details abstracted out

The Algorithm

- Up-flow: U_i raises received values to the power of the values (x_i, α_i) and forwards to U_{i+1}

- Down-flow: U_n processes the last up-flow and broadcasts

α_1, x_1

$[g_1, g_1^{x_1}]_{pw}$

α_2, x_2

$[g_3^{x_2 x_3}, g_3^{x_1 x_3}]_{pw}$

$[g_2^{x_2}, g_2^{x_1}, g_2^{x_1 x_2}]_{pw}$

$sk = H((g^{\alpha_1 \alpha_2 \alpha_3})^{x_1 x_2 x_3})$

α_3, x_3

Security Measurement (AKE) : Dictionary Attacks

- Theorem

$$\text{Adv}^{ake}(T, q_s, q_e) \leq 2q_s / N + 2q_s \cdot Adv^{mddh}(T')$$
$$+ 2q_h \cdot \text{Succ}^{gcdh}(T') + \text{«negligible terms»}$$

$$T' \leq T + n(3q_s + q_e) \cdot T_{exp}(k)$$

- Ideal-cipher assumption

- Security against dictionary attacks
  — the adversary's advantage grows essentially with the ratio of interactions (number of send-queries) to the number of password

Defining the Games

- Game 0 : the adversary plays against the oracles in order to defeat the AKE-security of the protocol

- Game 1: we delete the executions in which the adversary has guessed the password

- Game 2 : we simulate the protocol flows using the elements from a GCDH-tuple

- Game 3 : we simulate the protocol flows using the elements from a GCDH-tuple whose value $g^{x_1 \cdot \cdot x_n}$ is unknown

- Game 4 : we answer at random to the Test-query and thus fix the adversary's probability of correctly guessing the bit b to be 1/2.

- Proba[Adversary has guessed the password] = $2q_s / N + q_s \cdot Adv^{mddh}(T')$

Conclusion and Future Work

- Summary
  - A security model for security against dictionary attacks
  - A password group key agreement protocol
  - A proof of security

- Limitations
  - Ideal-hash and ideal-cipher assumptions

- Work in Progress
  - "Key Agreement for Heterogeneous Mobile Devices",
  - "Proofs of Security for the IEEE P1363 AuthA Protocol and Extensions"